

17. 02 2005



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 23 DEC. 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets


Martine PLANCHE

BEST AVAILABLE COPY

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

REMISE DES PIÈCES DATE 23 DEC 2003 LIEU 75 INPI PARIS 34 SP N° D'ENREGISTREMENT 0315321 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 23 DEC. 2003		11 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE CABINET PLASSERAUD 65/67 rue de la Victoire 75440 PARIS CEDEX 09	
Vos références pour ce dossier (facultatif)			
Confirmation d'un dépôt par télécopie		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
<i>Demande de brevet initiale</i> <i>ou demande de certificat d'utilité initiale</i>		N° _____ Date _____ N° _____ Date _____	
Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>		<input type="checkbox"/> N° _____ Date _____	
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) PROCEDE ET DISPOSITIF DE TRANSMISSION D'INFORMATIONS AVEC VERIFICATION DES ERREURS DE TRANSMISSION INVOLONTAIRES OU VOLONTAIRES			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation _____ Date _____ N° _____ Pays ou organisation _____ Date _____ N° _____ Pays ou organisation _____ Date _____ N° _____ <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR (Cochez l'une des 2 cases)		<input checked="" type="checkbox"/> Personne morale <input type="checkbox"/> Personne physique	
Nom ou dénomination sociale		EADS TELECOM	
Prénoms			
Forme juridique		Société par Actions Simplifiée	
N° SIREN		414848988	
Code APE-NAF			
Domicile ou siège	Rue	Bue Jean-Pierre Timbaud Batiment Jean-Pierre Timbaud 78180 MONTIGNY LE BRETONNEUX	
	Code postal et ville		
	Pays		
Nationalité		FRANCE	
N° de téléphone (facultatif)		Française N° de télécopie (facultatif)	
Adresse électronique (facultatif)			
<input type="checkbox"/> S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»			

REMISE DES PIÈCES DATE 23 DEC 2003 LIEU 75 INPI PARIS 34 SP N° D'ENREGISTREMENT 0315321 NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI BFF020220	DB 540 W / 210502
6 MANDATAIRE (s'il y a lieu)		7 INVENTEUR (S)	
Nom Prénom Cabinet ou Société N° de pouvoir permanent et/ou de lien contractuel Adresse Rue Code postal et ville Pays N° de téléphone (facultatif) N° de télécopie (facultatif) Adresse électronique (facultatif)		Les inventeurs sont nécessairement des personnes physiques <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)	
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/>	
Paiement échelonné de la redevance (en deux versements)		Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt <input type="checkbox"/> Oui <input type="checkbox"/> Non	
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requis pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Obtenue antérieurement à ce dépôt pour cette invention (joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence) : AG	
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		<input type="checkbox"/> Cochez la case si la description contient une liste de séquences	
Le support électronique de données est joint La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		<input type="checkbox"/> <input type="checkbox"/>	
Si vous avez utilisé l'imprimé «Suite», Indiquez le nombre de pages jointes			
11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) Stéphane VERDURE 97-0901		VISA DE LA PRÉFECTURE OU DE L'INPI 	

PROCEDE ET DISPOSITIF DE TRANSMISSION D'INFORMATIONS AVEC VERIFICATION DES ERREURS DE TRANSMISSION INVOLONTAIRES OU VOLONTAIRES

La présente invention concerne un procédé et un dispositif pour permettre la vérification de l'intégrité et l'authentification de l'origine d'un signal de radiocommunications.

Elle se rapporte au domaine des radiocommunications, et plus
5 particulièrement des systèmes de radiocommunications mobiles professionnelles ou systèmes PMR (de l'anglais "Professional Mobile Radiocommunication").

Elle trouve des applications dans les émetteurs radiofréquences qui sont compris aussi bien dans les stations de base que dans les terminaux
10 mobiles d'un tel système.

Dans le contexte des systèmes PMR, la vérification de l'intégrité et l'authentification de l'origine d'un signal consistent à vérifier que le signal n'a pas été volontairement corrompu par un tiers malveillant. Le but est, pour chaque terminal mobile, de vérifier que le signal radio reçu provient d'une
15 station de base du système, et non d'une station de base pirate, et, réciproquement, pour chaque station de base de vérifier qu'un signal radio reçu provient d'un terminal mobile du système, et non d'un terminal mobile pirate. Dit autrement, ce contrôle permet de détecter les attaques contre le système qui consistent à émettre un message ayant les caractéristiques
20 (synchronisation, format de protocole, codage, etc.) d'un message radio du système, mais en étant néanmoins un faux message ou un message falsifié par un adversaire ayant intercepté un message authentique.

Un faux message et un message falsifié peuvent être regardés comme des messages contenant des erreurs volontaires introduites par un tiers
25 malveillant pendant la transmission, par opposition avec des erreurs involontaires dues aux mauvaises conditions de la transmission radio.

La détection d'erreurs involontaires lors des transmissions radio est permise par l'utilisation d'un code de redondance cyclique ou CRC (de l'anglais "Cyclic Redundancy Code"), qui est formé par des bits de vérification des
30 erreurs de transmission transmis dans chaque trame radio en étant associé avec un message d'informations utiles.

La technique du CRC est largement utilisée dans les systèmes de radiocommunications pour la transmission de la voix ou de données. Les CRC sont des fonctions linéaires bien connues, dont un certain nombre est normalisé. Ainsi, pour transmettre un message M , on calcule le code $CRC(M)$, puis on code (codage de canal) et on transmet l'information $M+CRC(M)$ dans une trame. A la réception, l'information $M'+(CRC(M))'$ reçue dans une trame est décodée (décodage de canal), et doit vérifier la condition supplémentaire $CRC(M')=(CRC(M))'$ pour qu'on puisse considérer que $M'=M$. On notera que la technique permet de détecter les erreurs involontaires mais pas de les corriger : un message corrompu n'est simplement pas pris en compte.

Cette technique a été adoptée sans modification par de nombreux systèmes PMR (par exemple TETRAPOL, TETRA, etc.), pour protéger la transmission des trames radio contre les erreurs involontaires dues aux mauvaises conditions radios.

Cette technique ne permet toutefois pas au récepteur de détecter les erreurs volontaires introduites par un tiers malveillant. En effet, une caractéristique du CRC est d'être connu, en sorte qu'un adversaire peut remplacer/modifier le message M par/en un message N , puis calculer le code $CRC(N)$ avec le CRC parfaitement connu, et enfin coder et transmettre l'information $N+CRC(N)$ dans une trame sans que le ou les récepteurs ne détectent la moindre anomalie.

La technique du CRC est complétée dans des systèmes comme le GSM ("Global System for Mobiles") ou les systèmes selon la norme IEEE 802.11, en appliquant un chiffrement linéaire (CL) à l'information $M+CRC(M)$ pour obtenir une information de même taille $Z=CL((M + CRC(M)))$, qui est effectivement codée et transmise dans la trame. Ce complément semble apporter une réponse partielle au besoin d'intégrité car, la trame étant chiffrée, un tiers malveillant ne connaît pas le message M et il ne peut pas lui substituer un message falsifié.

Mais, en fait, il est toujours possible de transmettre un faux message car le chiffrement et le CRC sont tous les deux linéaires. Ainsi, soit un mot d'information D alors l'information $Z+CL(D+CRC(D))$ est en réalité égale à

l'information $CL(((M+D)+CRC(M+D)))$, et constitue un faux message qu'un attaquant sait construire et qui reste valide au regard des récepteurs.

La technique du CRC complétée par un chiffrement linéaire présente donc toujours l'inconvénient majeur que le récepteur ne peut pas détecter des erreurs volontaires introduites par un tiers malveillant.

En fait, la détection d'erreurs volontaires serait rendue possible avec l'introduction d'un mécanisme supplémentaire de scellement ("Sealing" en anglais), qui présenterait cependant l'inconvénient de réduire la bande passante utile.

En effet, une fonction de scellement produit un sceau ("Seal" en anglais) noté $S(M)$ dans la suite, sur un nombre de bits déterminé, qui devrait alors être codé et transmis dans la trame en association avec le message d'origine M et le code $CRC(M)$.

L'objet de la présente invention est de proposer un mécanisme de vérification de l'intégrité et d'authentification de l'origine d'un signal pour les communications dans un système de radiocommunications, permettant de pallier les inconvénients de l'art antérieur précités.

Ce but est atteint, selon un premier aspect de l'invention, grâce à un procédé de transmission d'informations avec vérification des erreurs de transmission, suivant lequel un message d'informations utiles est transmis dans une trame déterminée en étant associé à un nombre déterminé p de bits de vérification des erreurs de transmission qui sont également transmis dans ladite trame déterminée, et suivant lequel un nombre déterminé p_1 desdits p bits de vérification des erreurs de transmission forment un sceau obtenu à partir d'une fonction de scellement déterminée, où p_1 est un nombre inférieur ou égal à p .

Dit autrement, on remplace par un sceau, aussi appelé signature ou condensé (en anglais "digest"), tout ou partie des bits de vérification des erreurs qui forment habituellement un code de redondance cyclique associé au message. Ce remplacement permet de disposer d'un élément permettant la détection d'erreurs volontaires, c'est-à-dire la vérification de l'intégrité et l'authentification d'origine des messages, sans affecter le débit d'informations utiles (bande passante) du système par rapport à un mécanisme de vérification

des erreurs involontaires par CRC selon l'art antérieur. Cet élément est produit à sens unique, à l'aide d'une clé d'intégrité utilisée par la fonction de scellement.

Il s'ensuit que l'invention permet avantageusement l'introduction d'un
5 mécanisme de vérification d'intégrité et d'authentification d'origine des messages transmis dans un système existant, dans lequel aucune bande passante n'aurait été réservée à cet effet.

Dans un mode de mise en œuvre préféré, le sceau est formé de la totalité desdits p bits de vérification des erreurs de transmission, c'est-à-dire
10 que $p_1 = p$. Les meilleures performances en terme d'intégrité sont ainsi obtenues.

Néanmoins, dans d'autres modes de mise en œuvre, le sceau n'est formé que d'une partie desdits p bits de vérification des erreurs de transmission, c'est-à-dire que $p_1 < p$. Les $p - p_1$ bits restants peuvent alors former
15 un code de redondance cyclique (CRC). On conserve ainsi un CRC pour la détection spécifiquement des erreurs involontaires.

Pour préserver l'inviolabilité de la clé d'intégrité, les p_1 bits de vérification des erreurs de transmission formant le sceau peuvent être calculés au niveau de la couche de protocole MAC (de l'anglais "Medium Access
20 Control"), puis être délivrés à un codeur de canal au niveau de la couche physique.

Un deuxième aspect de l'invention se rapporte à un dispositif de transmission d'informations avec vérification des erreurs de transmission, comprenant des moyens pour transmettre dans une trame déterminée un
25 message d'informations utiles associé à un nombre déterminé p de bits de vérification des erreurs de transmission également transmis dans ladite trame déterminée, et des moyens pour obtenir un sceau à partir d'une fonction de scellement déterminée, qui forme un nombre déterminé p_1 desdits p bits de
vérification des erreurs de transmission, où p_1 est un nombre inférieur ou égal
30 à p .

Un troisième aspect de l'invention se rapporte encore à un équipement de radiocommunications comprenant un dispositif selon le deuxième aspect.

Un tel équipement peut en particulier être un terminal mobile ou une station de base d'un système de radiocommunications, par exemple un système PMR.

D'autres caractéristiques et avantages de l'invention apparaîtront encore à la lecture de la description qui va suivre. Celle-ci est purement illustrative et doit être lue en regard des dessins annexés sur lesquels :

- la figure 1 montre un exemple de structure de trame utilisée avec un procédé de transmission d'information selon l'art antérieur ;

- la figure 2 montre un premier exemple de structure de trame utilisée avec un procédé selon l'invention ;

- la figure 3 montre un second exemple de structure de trame utilisée avec un procédé selon l'invention ;

- la figure 4 est un schéma synoptique d'une chaîne d'émission radio pour la mise en œuvre du procédé selon l'invention ;

- la figure 5 est un schéma synoptique d'une chaîne de réception radio pour la mise en œuvre du procédé selon l'invention ;

- la figure 6 est un diagramme d'étapes illustrant le calcul de sceau selon un premier mode de mise en œuvre du procédé selon l'invention ; et,

- la figure 7 est un diagramme d'étapes illustrant le calcul de sceau selon un second mode de mise en œuvre du procédé selon l'invention.

La figure 1 montre une structure de trame classiquement utilisée pour la transmission d'informations par un procédé selon l'art antérieur.

La trame comprend un message d'informations utiles, référencé M dans la suite, codé sur un nombre déterminé n de bits. Elle comprend également un nombre déterminé p de bits de vérification des erreurs de transmission qui sont associés au message M. Ces p bits forment en général un code à redondance cyclique, ci-après référencé CRC(M). Enfin, la trame comprend un nombre déterminé q de bits de bourrage ("padding" en anglais).

Dans un système de radiocommunications, une telle trame est émise dans une salve ("burst", en anglais) et est de ce fait de taille relativement réduite. Dans un exemple, $n=92$, $p=10$, et $q=3$, en sorte que la trame comprend au total 105 bits.

Le schéma de la figure 2 illustre un premier exemple de structure de trame utilisable avec un procédé selon l'invention.

Dans cet exemple, un nombre déterminé p_1 parmi les p bits de vérification des erreurs de transmission forment un sceau obtenu à partir d'une fonction de scellement déterminée où p_1 est un nombre inférieur ou égal à p . Dans cet exemple, les p_2 autres bits de vérification des erreurs de transmission, où $p_2 = p - p_1$, forment toujours un code de redondance cyclique. Les n bits du message M , ainsi que les q bits de bourrage ne sont pas modifiés par rapport à la structure de trame selon l'art antérieur qui est représentée à la figure 1.

Dit autrement, le procédé selon l'invention consiste dans cet exemple à remplacer le CRC sur p bits par un CRC sur p_2 bits, et à introduire un sceau sur p_1 bits, où $p_1 + p_2 = p$.

Un second exemple de structure de trame utilisable avec un procédé selon l'invention, qui est illustré à la figure 3, se distingue du premier exemple ci-dessus en ce que le sceau est formé de la totalité des p bits de vérification des erreurs de transmission associés au message M . Dit autrement, en utilisant la notation précédente, $p_1 = p$ et $p_2 = 0$.

Le fait d'introduire un scellement permet de détecter les erreurs involontaires (rôle habituel du CRC) mais aussi de lutter contre la falsification volontaire du message par un adversaire ayant intercepté le message. On note que, compte tenu des conditions de transmission radio, un élément protégeant contre les erreurs involontaires est de toute façon obligatoire, et le fait de l'implémenter (au moins en partie) sous la forme d'un sceau de même taille (au plus) qu'un CRC, ne réduit pas la bande passante utile par rapport aux implémentations par CRC connues.

La figure 4 montre schématiquement une chaîne d'émission radio pour la mise en œuvre du procédé selon l'invention. Un tel émetteur est par exemple compris dans les terminaux mobiles et dans les stations de base d'un système de radiocommunications implémentant l'invention.

Un codeur de source 31, généralement appelé Codec, fournit une suite de messages d'informations utiles M à partir d'un signal analogique, par exemple un signal de parole. Les messages M sont des messages numériques d'informations vocales codées sur n bits. En variante, les messages M sont des messages de données numériques provenant d'une source de données

quelconque. Les messages M sont transmis à un module 32 de calcul de sceau, qui reçoit aussi une clé d'intégrité K stockée dans une mémoire protégée 33. La clé K est secrète. A partir d'un message M et de la clé K , le module 32 calcule un sceau $S(M)$ à partir d'une fonction de scellement S déterminée. Le sceau $S(M)$ et le message M sont fournis en entrée d'un codeur de canal 34 qui les introduit dans la structure de trame représentée à la figure 2 ou à la figure 3. Dans le cas de la structure de trame selon la figure 2, le codeur de canal 34 réalise également le calcul du code $CRC(M)$, et l'introduit dans la structure de trame. L'information $M+S(M)$, où le cas échéant l'information $M+S(M)+CRC(M)$, est transmise à un module d'embrouillage 35, puis à un modulateur 36, puis à un module d'émission radio 37, pour être émise sur le canal de transmission à l'intérieur d'une salve.

La figure 5 montre un schéma synoptique de la chaîne de réception d'un équipement pour la mise en œuvre du procédé selon l'invention.

Un signal radio est reçu par un récepteur radio 47, puis transmis à un démodulateur 46, et ensuite à un module de désembrouillage 45 qui délivre une information $M'+S(M)'$, voire le cas échéant l'information $M'+S(M)'+CRC(M)'$. Cette information est transmise à un décodeur de canal 44, qui récupère l'information M' correspondant au message tel que reçu, ainsi que l'information $S(M)'$ correspondant au sceau tel que reçu.

Les informations M' et $S(M)'$ sont transmises à un module de vérification de sceau 42. Lorsqu'un mode de réalisation avec une structure de trame selon la figure 2 est mis en œuvre, on peut prévoir que les informations M' et $S(M)'$ soient transmises par le décodeur de canal 44 au module de vérification de sceau 42 uniquement en l'absence d'erreurs de transmission involontaires, c'est-à-dire lorsque $CRC(M)'=CRC(M)$.

Le module 42 a pour fonction de vérifier l'intégrité et d'authentifier l'origine du message M' reçu. A cet effet, il calcule le sceau $S(M)'$ et le compare au sceau $S(M)'$ reçu. En cas d'égalité, qui signifie que le message reçu n'est pas corrompu, ni par des erreurs involontaires ni par des erreurs volontaires, le module 42 transmet le message M' à un décodeur de source 41. Dans le cas contraire, qui signifie que le message reçu M' a été corrompu par l'introduction d'erreurs volontaires ou involontaires, le message M' n'est pas traité plus avant.

Pour effectuer le calcul du sceau $S(M)$, le module 42 utilise la même fonction de scellement S et la même clé secrète K que la chaîne d'émission. La clé K est stockée dans une mémoire protégée 43 de la chaîne de réception.

5 Ainsi qu'on l'aura compris, lorsque la chaîne d'émission de la figure 4 et la chaîne de réception de la figure 5 sont comprises dans un seul et même équipement radio, les modules 32 et 42 possèdent des éléments communs en tout ou partie. De même, les mémoires 33 et 43 peuvent être une seule et même mémoire.

10 Les modules 32, 34-36, 42 et 43-46 sont des exemples réalisés sous la forme de modules essentiellement logiciels.

Du point de vue des protocoles mis en œuvre, les modules 32 et 42 interviennent avantageusement au niveau de la couche MAC ("Medium Access Control") alors que le codeur de canal 34 et les modules avals 35, 36 et 37 d'une part, ainsi que le décodeur de canal 44 et les modules amont 45, 46 et 15 47 d'autre part, interviennent au niveau de la couche physique. De cette façon, la clé secrète K n'apparaît qu'au niveau de la couche MAC seulement, alors que les bits de vérification des erreurs de transmission apparaissent au niveau de la couche physique. Il s'ensuit que l'inviolabilité de la clé secrète K est plus facile à préserver.

20 Un premier mode de calcul du sceau $S(M)$ est illustré par le diagramme d'étapes de la figure 6.

Dans une première étape 61, le module 32 utilise une fonction de scellement connue en elle-même, produisant un résultat sur un nombre déterminé m de bits, où m peut être supérieur à p_1 , à partir de la clé secrète K 25 et du message M . Ce résultat est noté $S(M)$ / m bits dans la suite et à la figure.

La fonction de scellement peut être une fonction de hachage à clé, aussi appelée fonction de type Hash-MAC ou HMAC à clé (de l'anglais "keyed Hash Message Authentication Code"). Par exemple, cette fonction peut être sélectionnée parmi les fonctions connues suivantes : la fonction MD5 pour 30 laquelle $m=128$, la fonction SHA-1 pour laquelle $m=160$, la fonction SHA-256 pour laquelle $m=256$... Ces fonctions connues ont été publiées et sont disponibles auprès du NIST ("National Institute of Standard Technologies").

En variante, il peut s'agir d'une fonction de hachage spécifique, conçue à partir d'un algorithme de chiffrement par blocs. Un tel algorithme est par exemple l'algorithme TDES ("Triple DES"), ou l'algorithme AES ("Advanced Encryption Standard") qui a été publié pour remplacer l'algorithme DES ("Data Encryption System").

Selon une propriété des fonctions de scellement envisagées ci-dessus, une modification d'un bit dans le message M occasionne, en moyenne, la modification d'un bit sur deux dans le résultat $S(M)$ / m bits.

Dans une étape 62, le sceau $S(M)$ sur $p1$ bits, noté $S(M)$ / $p1$ bits à la figure, est obtenu en tronquant à $p1$ bits le résultat $S(M)$ / m bits de la fonction de scellement obtenu à l'étape 61. De cette manière, le sceau $S(M)$ présente bien le nombre maximum $p1$ de bits disponibles pour sa transmission dans la trame.

Les bits du résultat $S(M)$ / m bits de la fonction de scellement obtenu à l'étape 61 étant équiprobables, selon une probabilité des fonctions de hachage envisagées ci-dessus, le sceau $S(M)$ / $p1$ bits résultant de la troncature peut être une séquence quelconque de $p1$ bits du résultat $S(M)$ / m bits. Le plus simple est de sélectionner les bits les plus significatifs ou MSB (de l'anglais "Most Significant Bits") ou les bits les moins significatifs ou LSB (de l'anglais "Least Significant Bits") du résultat $S(M)$ / m bits. Bien entendu, les mêmes bits doivent être sélectionnés coté émetteur et coté récepteur.

L'avantage de ce premier mode de mise en œuvre est de permettre l'utilisation d'une fonction de scellement quelconque, avec un sceau de taille ramenée à la taille voulue en tronquant le résultat de cette fonction si nécessaire. En contrepartie on peut avoir des propriétés de détection d'erreurs involontaires différentes de celles obtenue avec un CRC linéaire, pour certains types d'erreurs. En effet, bien que la détection des erreurs soit la même pour une probabilité des erreurs uniforme sur l'ensemble des messages transmis, elle sera moins favorable en cas de probabilité non-uniforme.

C'est pourquoi un second mode de calcul du sceau $S(M)$, illustré par le diagramme d'étapes de la figure 7, prévoit l'utilisation d'une fonction de scellement spécifique.

Cette fonction est adaptée pour garantir la détection d'erreurs involontaires de la même façon qu'un CRC. On propose une fonction mathématique comprenant la combinaison, d'une part d'une fonction GPA de génération d'un pseudo-aléa, et d'autre part d'un code non-linéaire CNL. La fonction GPA génère, à partir d'une clé secrète K et d'une variable d'initialisation déterminée, une suite de chiffrement de longueur quelconque, par exemple d'au plus 2^{64} valeurs distinctes. Le code CNL doit avoir une distance de Hamming égale ou supérieure à celle d'un CRC habituellement utilisé dans le type d'applications visé. A tailles égales on sait qu'il existe un code non-linéaire qui vérifie cette propriété.

Avec une fonction mathématique de ce type, la détection des erreurs volontaires résulte de la fonction GPA, et celle des erreurs involontaires résulte du code non-linéaire CNL. On optimise les performances en choisissant un code non-linéaire CNL ayant des propriétés pour garantir un bon hachage.

A partir d'un message M à sceller avec une clé secrète K, un exemple de telle fonction comprend les calculs suivants.

Dans une première étape 71, on réalise le calcul d'une variable X à l'aide de la fonction GPA appliquée à la clé K et à une première variable d'initialisation VI1, de telle manière que :

$$X = \text{GPA}(\text{VI1}, K) \quad (1)$$

Puis dans une deuxième étape 72, on calcule une information Y(M) à l'aide d'une matrice linéaire A_X construite à partir de la variable X, et appliquée au message M, de telle manière que :

$$Y(M) = A_X(M) \quad (2)$$

Dans une troisième étape 73, qui peut être effectuée parallèlement à ou avant les étapes 71 et 72, on réalise le calcul d'une variable Z à l'aide de la fonction GPA appliquée à la clé K et à une seconde variable d'initialisation VI2, de telle manière que :

$$Z = \text{GPA}(\text{VI2}, K) \quad (3)$$

Enfin, dans une dernière étape 74, qui intervient nécessairement après les étapes 72 et 73, on calcule le sceau S(M) à l'aide d'une matrice linéaire A_Z

construite à partir de la variable Z, et appliquée à l'information Y(M), de telle manière que :

$$S(M) = A_Z (CNL(Y(M))) \quad (4)$$

- 5 Ainsi qu'il apparaîtra immédiatement à l'Homme du métier, il existe une pluralité de fonctions GPA, de codes non-linéaires CNL et de matrices linéaires A satisfaisant aux buts recherchés.

REVENDEICATIONS

1. Procédé de transmission d'informations avec vérification des erreurs de transmission, suivant lequel un message (M) d'informations utiles est transmis dans une trame déterminée en étant associé à un nombre déterminé p de bits de vérification des erreurs de transmission (CRC;S) également
5 transmis dans ladite trame déterminée,

et suivant lequel un nombre déterminé p_1 desdits p bits de vérification des erreurs de transmission forment un sceau (S) obtenu à partir d'une fonction de scellement déterminée, où p_1 est un nombre inférieur ou égal à p .

2. Procédé selon la revendication 1 suivant lequel le sceau (S) est
10 formé de la totalité desdits p bits de vérification des erreurs de transmission.

3. Procédé selon la revendication 1 suivant lequel le sceau n'est formé que d'une partie desdits p bits de vérification des erreurs de transmission, les $p-p_1$ bits restants formant un code de redondance cyclique (CRC).

4. Procédé selon l'une quelconque des revendications précédentes,
15 suivant lequel les p_1 bits de vérification des erreurs de transmission sont calculés au niveau de la couche de protocole MAC, puis sont délivrés à un codeur de canal au niveau de la couche physique.

5. Procédé selon l'une quelconque des revendications précédentes
20 suivant lequel le sceau est obtenu en tronquant à p_1 le résultat de la fonction de scellement qui est obtenu sur un nombre de bits supérieur à p_1 .

6. Procédé selon la revendication 5, suivant lequel la fonction de scellement est de type Hash-MAC à clé, avec une fonction de hachage sélectionnée dans le groupe comprenant la fonction MD5, la fonction SHA-1, la fonction SHA-256 et des fonctions de scellement conçues à partir d'un
25 algorithme de chiffrement par blocs.

7. Procédé selon l'une quelconque des revendications 1 à 4, suivant lequel le résultat de la fonction de scellement est obtenu directement sur p_1 bits.

8. Procédé selon la revendication 7, suivant lequel la fonction de scellement comprend la combinaison d'une fonction de génération de pseudo-aléa (GPA) et d'une fonction de codage non linéaire (CNL).

5 9. Dispositif de transmission d'informations avec vérification des erreurs de transmission, comprenant des moyens pour transmettre dans une trame déterminée un message (M) d'informations utiles associé à un nombre déterminé p de bits de vérification des erreurs de transmission (CRC,S) également transmis dans ladite trame déterminée,

10 et des moyens pour obtenir un sceau (S) à partir d'une fonction de scellement déterminée, qui forme un nombre déterminé p_1 desdits p bits de vérification des erreurs de transmission, où p_1 est un nombre inférieur ou égal à p .

10. Dispositif selon la revendication 9, dans lequel le sceau est formé de la totalité desdits n bits de vérification des erreurs de transmission.

15 11. Dispositif selon la revendication 9, dans lequel le sceau n'est formé que d'une partie desdits p bits de vérification des erreurs de transmission, les $p-p_1$ bits restants formant un code de redondance cyclique (CRC).

20 12. Dispositif selon l'une quelconque des revendications 9 à 11, comprenant des moyens pour calculer les p_1 bits de vérification des erreurs de transmission au niveau de la couche de protocole MAC, ainsi qu'un codeur de canal auquel lesdits p_1 bits sont délivrés au niveau de la couche physique.

13. Dispositif selon l'une quelconque des revendications 9 à 12, comprenant des moyens pour obtenir le sceau en tronquant à p_1 le résultat de la fonction de scellement qui est obtenu sur un nombre de bits supérieur à p_1 .

25 14. Dispositif selon la revendication 13, dans lequel la fonction de scellement est de type Hash-MAC à clé; avec une fonction de hachage sélectionnée dans le groupe comprenant la fonction MD5, la fonction SHA-1, la fonction SHA-256 et des fonctions de scellement conçues à partir d'un algorithme de chiffrement par blocs.

8. Procédé selon la revendication 7, suivant lequel la fonction de scellement comprend la combinaison d'une fonction de génération de pseudo-aléa (GPA) et d'une fonction de codage non linéaire (CNL).

5 9. Dispositif de transmission d'informations avec vérification des erreurs de transmission, comprenant des moyens pour transmettre dans une trame déterminée un message (M) d'informations utiles associé à un nombre déterminé p de bits de vérification des erreurs de transmission (CRC,S) également transmis dans ladite trame déterminée,

10 et des moyens pour obtenir un sceau (S) à partir d'une fonction de scellement déterminée, qui forme un nombre déterminé p_1 desdits p bits de vérification des erreurs de transmission, où p_1 est un nombre inférieur ou égal à p .

10. Dispositif selon la revendication 9, dans lequel le sceau est formé de la totalité desdits p bits de vérification des erreurs de transmission.

15 11. Dispositif selon la revendication 9, dans lequel le sceau n'est formé que d'une partie desdits p bits de vérification des erreurs de transmission, les $p-p_1$ bits restants formant un code de redondance cyclique (CRC).

20 12. Dispositif selon l'une quelconque des revendications 9 à 11, comprenant des moyens pour calculer les p_1 bits de vérification des erreurs de transmission au niveau de la couche de protocole MAC, ainsi qu'un codeur de canal auquel lesdits p_1 bits sont délivrés au niveau de la couche physique.

13. Dispositif selon l'une quelconque des revendications 9 à 12, comprenant des moyens pour obtenir le sceau en tronquant à p_1 le résultat de la fonction de scellement qui est obtenu sur un nombre de bits supérieur à p_1 .

25 14. Dispositif selon la revendication 13, dans lequel la fonction de scellement est de type Hash-MAC à clé, avec une fonction de hachage sélectionnée dans le groupe comprenant la fonction MD5, la fonction SHA-1, la fonction SHA-256 et des fonctions de scellement conçues à partir d'un algorithme de chiffrement par blocs.

15. Dispositif selon l'une quelconque des revendications 9 à 12, comprenant des moyens pour obtenir le résultat de la fonction de scellement directement sur p1 bits.

5 16. Dispositif selon la revendication 15, dans lequel la fonction de scellement comprend la combinaison d'une fonction de génération de pseudo-aléa (GPA) et d'une fonction de codage non linéaire (CNL).

17. Equipement de radiocommunications comprenant un dispositif selon l'une quelconque des revendications 9 à 16.

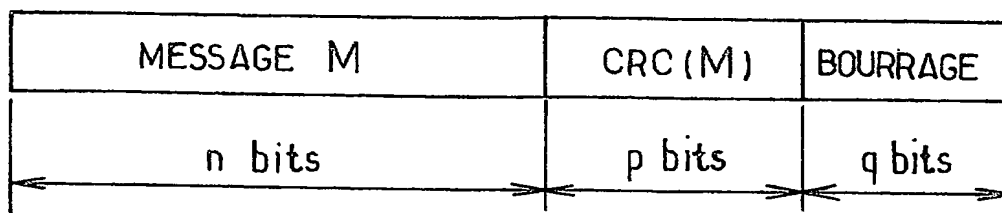


FIG.1.

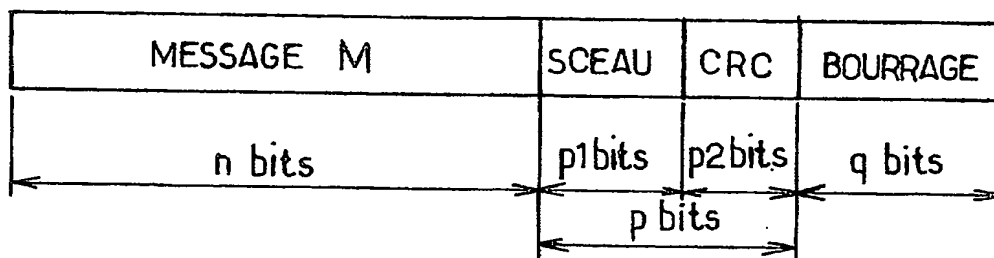


FIG.2.

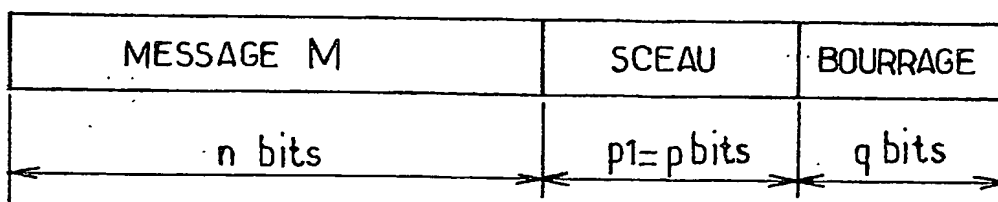


FIG.3.

FIG.4.

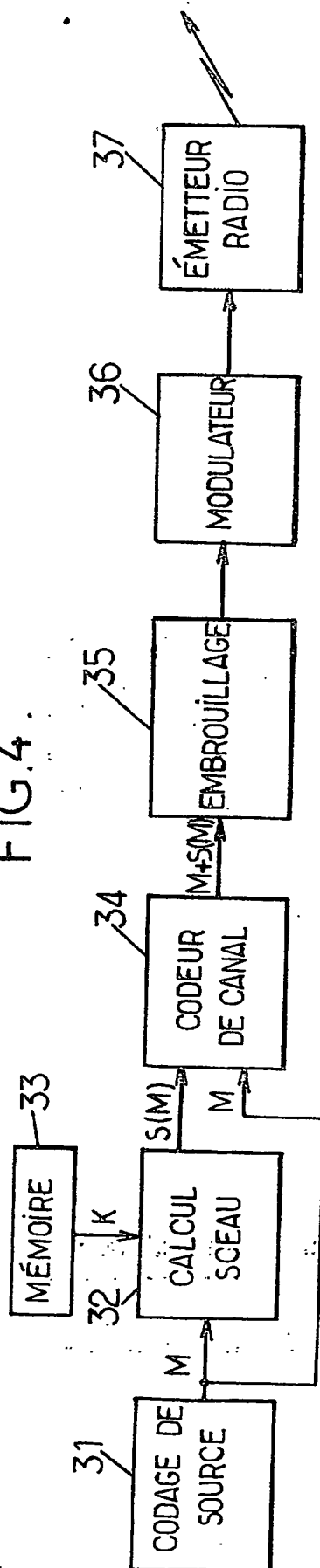


FIG.5.

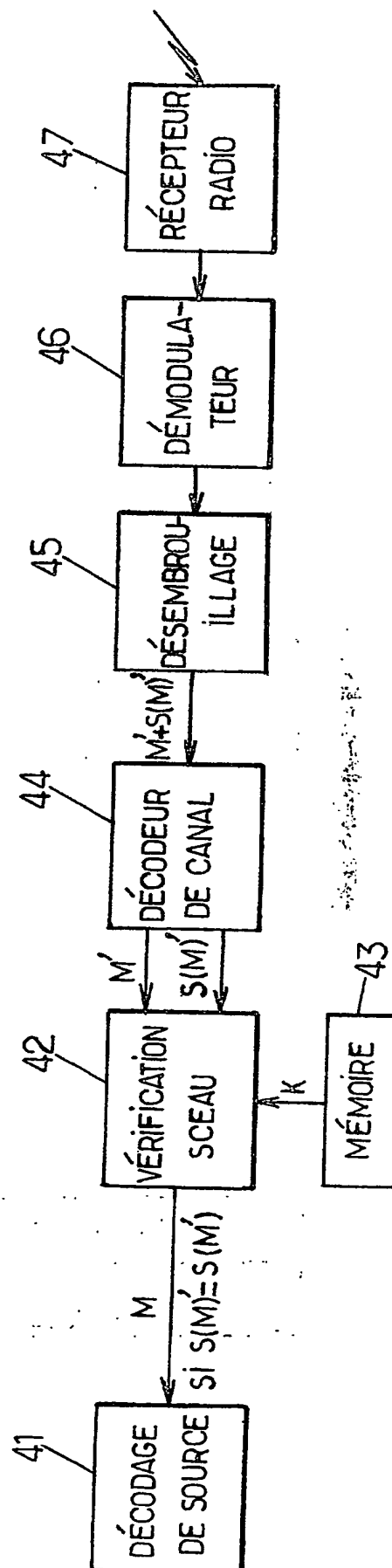


FIG. 6.

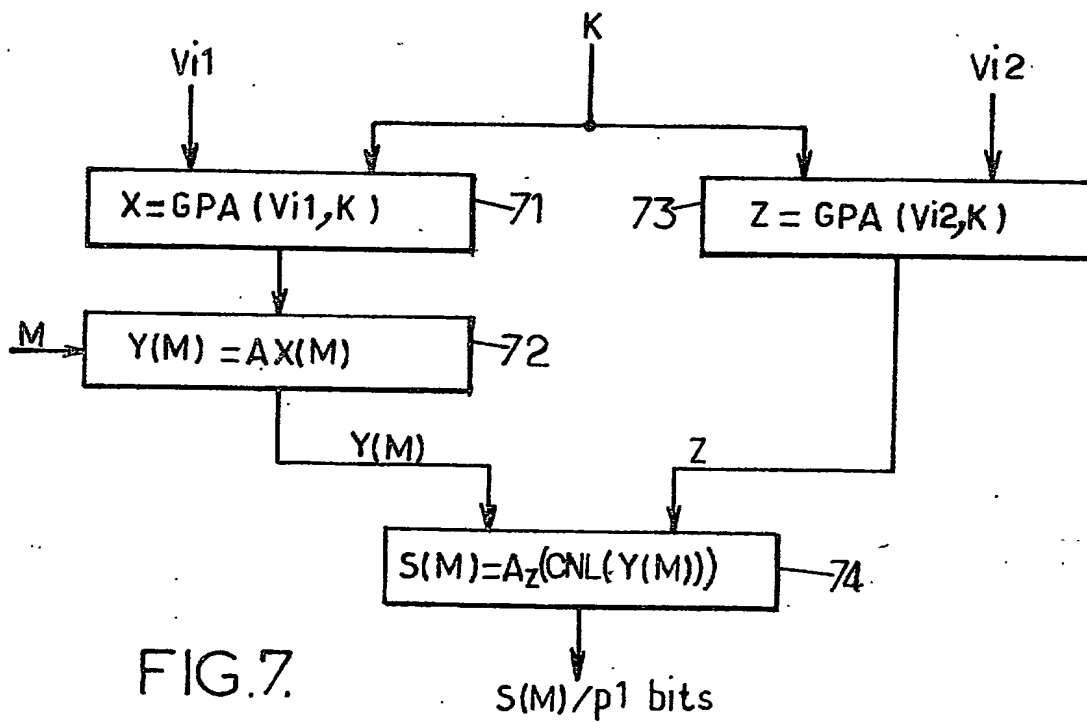
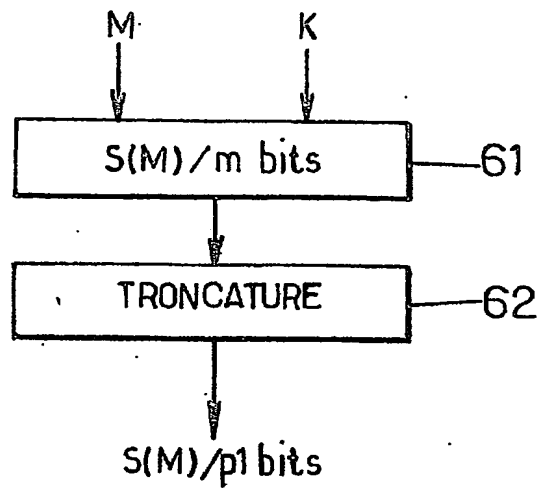


FIG. 7.

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1 / 1
(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)



Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 270601

Vos références pour ce dossier (facultatif)			
N° D'ENREGISTREMENT NATIONAL		0315 381	
TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
PROCÉDE ET DISPOSITIF DE TRANSMISSION D'INFORMATIONS AVEC VERIFICATION DES ERREURS DE TRANSMISSION INVOLONTAIRES OU VOLONTAIRES			
LE(S) DEMANDEUR(S) :			
EADS TELECOM			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) :			
<input checked="" type="checkbox"/> 1	Nom	MOUFFRON Marc	
	Prénoms		
	Adresse	Rue	16 rue Lamartine 78470 SAINT REMY LES CHEVREUSES
		Code postal et ville	FRANCE
	Société d'appartenance (facultatif)		
<input checked="" type="checkbox"/> 2	Nom	TENKES Jean-Michel	
	Prénoms		
	Adresse	Rue	1380 Rue de la Bretechele 78370 PLAISIR FRANCE
		Code postal et ville	FRANCE
	Société d'appartenance (facultatif)		
<input checked="" type="checkbox"/> 3	Nom		
	Prénoms		
	Adresse	Rue	
		Code postal et ville	
	Société d'appartenance (facultatif)		
S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		Le 23 décembre 2003 CABINET PLASSERAUD Stéphane VERDURE 97-0901 	

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP04/014901

International filing date: 22 December 2004 (22.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: FR
Number: 03/15321
Filing date: 23 December 2003 (23.12.2003)

Date of receipt at the International Bureau: 25 February 2005 (25.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.